IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Bruce L. Davis
Application No.: 10/086,180
Filed: February 25, 2002
For: DISTRIBUTION AND USE OF TRUSTED PHOTOS
Examiner: D Lazaro
Date: April 18, 2008

Art Unit 2155
Confirmation No. 1232

VIA ELECTRONIC FILING

SUBSTITUTE APPEAL BRIEF (SECOND[1])

Mail Stop: Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the *Notice of Appeal* filed June 1, 2007, the *Notice of Panel Decision from Pre-Appeal Brief Review* mailed February 13, 2008, and the *Notice of Non-Compliant Appeal Brief* mailed March 19, 2008.

The fee for filing the Appeal Brief has already been paid (with the March 12, 2008 filing). Please charge any other fee required, and/or any required extension of time, to deposit account 50-1071 (see transmittal letter).

[1] This application was earlier appealed in 2005; prosecution was re-opened following submission of the appeal brief.

I. REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 12979, Frames 813-814.

II. RELATED APPEALS AND INTERFERENCES

An earlier Final Rejection was appealed, but the Office re-opened prosecution upon filing of the first Appeal Brief.

III. STATUS OF CLAIMS

Claims 1-36 are pending.

Claims 1-15, 27, 28 and 33 are finally rejected and are appealed.

The remaining claims (including some dependent from claim 1) are withdrawn from consideration as being directed to a non-elected invention.

IV. STATUS OF AMENDMENTS

All prior amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The creation of identification documents, such as identification badges, has typically required that the individual being depicted sit for a picture. This is often an inconvenience, and may result in many different photos of an individual being taken for identification documents.[2]

Consider a different arrangement, as illustrated by the following scenario:

[2] Specification, page 1, lines 12-14.

An employment candidate will be interviewing at a new employer and needs an access badge.

The employer e-mails or otherwise sends the candidate an access code. The code is valid only for a certain time period on a given date (e.g., 9:00 a.m. – 11:00 a.m. on June 28, 1999).

Upon receiving the access code, the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo. The DMV has already encoded this photo with hidden watermark data, which points to a corresponding database record in a state-run server. (If that server is queried with data decoded from the photograph, the server accesses the database and may reply to the inquiring computer e.g., with a text string indicating the name of the person depicted by the photograph.)

The employment candidate incorporates the photo obtained from the DMV into an access badge. Using a software application on her home computer (which may be provided especially for such purposes, e.g., as part of an office productivity suite), the photo is dragged into an access badge template. The access code emailed from the employer is also provided to this application. On selecting "Print," an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo and her name, and is also digitally watermarked in accordance with the employer-provided access code.

The name printed on the badge is obtained (by the candidate's computer) from the DMV's server, in response to watermark data extracted from the photograph.

On the appointed day the candidate presents herself at the employer's building. At the exterior door lock, the candidate presents the home-printed badge to an optical sensor device, which reads the embedded building access code, checks it for authenticity and, if the candidate arrived within the permitted hours, unlocks the door.

Inside the building the candidate may encounter a security guard. Seeing an unfamiliar person, the guard may visually compare the photo on the badge with the candidate's face. Additionally, the guard can present the badge to a portable watermark reader device. The reader device decodes the watermark data from the card (e.g., from

the DMV photograph), interrogates the DMV's server with this data, and receives in reply the name of the person depicted in the photograph.

The guard checks the name returned from the DMV server with the name printed on the badge. On seeing that the printed and DMV-indicated names match, the security guard can let the candidate pass.

It will be recognized that the just-described arrangement offers very high security, yet this security is achieved with without the candidate ever previously visiting the employer, without the employer knowing what the candidate looks like, and by use of an access badge produced by the candidate herself.[3]

In accordance with one illustrative embodiment of the present invention, a trusted repository of images - such as an image archive maintained by a state motor vehicle licensing agency - is used to provide images for non-driver license applications. As needed, a user may electronically contact such an agency and solicit a copy of their driver license photo. The agency responds by sending an electronic version of the photo, which then can be incorporated, e.g., into an identification badge. Since the photograph comes from a trusted, independent source, it can be used in identification documents without requiring the individual to sit for another photo.[4]

In one particular arrangement (claim 1), an individual user[5] electronically contacts a governmental agency (such as a motor vehicle licensing agency),[6] and solicits an image depicting the user.[7] This image is stored in an archive maintained by the governmental agency.[8] In response, the user electronically receives back the solicited image from the agency,[9] and then prints a document (e.g., a photo identification document, such as a badge) incorporating the image.[10]

---

3 Specification, page 13, line 25 – page 15, line 4.
4 Specification, page 1, lines 15-21.
5 *See, e.g.,* specification, page 13, line 25 (*"…an employment candidate…"*).
6 *See, e.g.,* specification, page 13, lines 31-32 (*"…the state Department of Motor Vehicles"*).
7 *Ibid.* (*"…the latest copy of her driver's license photo."*).
8 *Ibid.* (the collection of DMV photos from which the web site provides the candidate's photo is an archive).
9 *Ibid.* (*"…the candidate downloads from the web site…"*).
10 *See, e.g.,* specification page 14, lines 3-8 (*"On selecting 'Print,' an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo…*).

The image provided by the government agency may have been processed with an identification code prior to provision to the user.[11] For example, the image may have been digitally watermarked with a plural-bit code that serves to identify the depicted individual.[12] (Such identification can be direct, or the code can comprise an index into a data structure[13] in which the individual user's name is stored.)

(Digital watermarking, sometimes termed "steganography," is the science of hiding secret information – often in some other data, and without leaving any apparent evidence of data alteration.[14] Digital watermarking can take many forms - several are detailed in patent documents incorporated-by-reference in the present specification.[15] One form of digital watermarking favored by the present Appellants involves making subtle changes to the luminance of pixels comprising a photograph to thereby encode a hidden multi-bit digital data payload. The changes are too slight to be perceptible to human viewers of the photo. But when such watermark-encoded printed photograph is sensed by an image sensor and computer analyzed, the encoded digital data can be recovered.)

In a second particular arrangement (independent claim 11), a governmental agency receives an electronic request for an archived personal image from an individual depicted in said image.[16] The image is then electronically transmitted to that individual.[17] Again, the image may be processed with an identification code (e.g., by digital watermarking) prior to transmission to the individual.[18]

---

11 *See, e.g.,* specification, page 13, lines 32-33.

12 *See, e.g.,* original claims 7, 8 (specification, page 46).

13 *See, e.g.,* specification, page 12, lines 4-6.

14 Digital watermarking is a well developed art that is not belabored in the present specification. Instead, the present specification incorporates-by-reference earlier patents and applications on the subject. *See, e.g.,* specification at page 7, lines 22-25; page 41, lines 26-33 (both subsequently amended by Amendment filed November 3, 2004), and incorporation-by-reference language at page 45, lines 1-2.

15 *Ibid.*

16 *See, e.g.,* specification at page 13, lines 31-32 ("*...the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo.*").

17 *Ibid.*

18 *See, e.g.,* specification, page 13, lines 32-33.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 5, 10, 11, 27 and 33 stand rejected under § 103 over Dellert (5,760,916).

Claims 4, 6-9, 12-15 and 28 stand rejected under § 103 over Dellert in view of Rhoads (5,841,886).

VII. ARGUMENT

1. Dellert 5,760,916

Dellert is a Kodak disclosure in which a consumer's film is submitted for developing, and Kodak posts digitized counterparts of the exposed pictures on the internet, for access by the consumer.

2. Claim 1 (§103 Dellert)

Claim 1 reads as follows:

> *1. A method of printing a trusted image, comprising:*
> *an individual user electronically contacting a governmental agency, soliciting an image depicting the user stored in an archive maintained by said governmental agency;*
> *electronically receiving said image from said contacted governmental agency; and*
> *printing a document incorporating said image.*

Two errors are made in rejecting the claim. First, an artisan would not have found the claimed method obvious. Second, the rejection relies on an error of law.

In Dellert, it is the consumer who owns the image. Kodak simply acts as a service provider – providing services to consumers who are proprietors of their respective images. Dellert teaches providing a consumer with electronic access to images *that the consumer owns*.

In contrast, image archives maintained by governmental agencies are not commercial repositories for images owned by consumers. The images are typically owned *by the government*. Nothing in Dellert would have led an artisan to grant consumer access to a *governmental* image archive.

Although hindsight may transform Dellert into the presently claimed method, it would not otherwise have been obvious to do so. Images from government archives – of the sort maintained by the US Department of State, or state motor vehicle departments, are not generally available for personal use. Absent a teaching otherwise, an artisan would not have considered such images to be available for non-governmental use. Absent hindsight, an artisan would not transform Dellert to yield the claimed invention. For this reason, the rejection should be reversed.

Reversal is also required because the Examiner's § 103 reasoning is based on legal error. The Examiner disregarded limitations expressed in the claim – asserting that language requiring a "governmental agency" are entitled to *no* patentable weight. Such limitations were dismissed as "descriptive,"[19] e.g.:

> said contacted governmental agency. It is desirable to allow users to remotely access images regardless of the type of agency storing those images (Col. 2 lines 11-27). The type of agency/entity is descriptive and does not form a patentable distinction.
>
> 7. With respect to Claim 2, Dellert further teaches it is the individual user who

"Descriptiveness" is not a ground for ignoring language found in the claim. Indeed, *all* claim limitations necessarily are descriptive – they serve to *describe* the claimed invention.

The Office cited no rule or MPEP policy in support of its action; none is evident. (This is not a case alleged to involve Computer-Related Nonstatutory Subject Matter, e.g., as detailed in MPEP § 2106.01.)

---

[19] Final Rejection, page 3, 6th and 5th lines from the bottom.

Absent compelling reason, each limitation in a claim should be given meaning. The Office failed to follow this rule. This failure is a second reason that the Final Rejection falls short of meeting the Office's *prima facie* burden under § 103, again requiring reversal.

3. Claim 2 (§103 Dellert)

Claim 2 stands or falls with the Dellert-based rejection of claim 1, from which it depends.

4. Claim 3 (§103 Dellert)

Claim 3 is allowable for its dependence from claim 1, and is also independently allowable. The claim reads:

> *3. The method of claim 1 in which said document is a photo identification document.*

The Final Rejection has not established *prima facie* obviousness because the Office misread the Dellert reference.

The Final Rejection states,[20] "*With respect to claim 3, Dellert further teaches said document is a photo identification document (Col. 3 lines 23-49).*"

Not so. Dellert has *no* teaching of a photo identification document. The cited passage reads:

[20] Final rejection, page 3, last two lines.

any failure in the system. In particular, the scanner location which was to communicate the images can be contacted to determine if the scanned images were in fact completely communicated to the hub station and if so, the particulars of such transmission, and to request a re-transmission if necessary. Additionally, the presence of a hub station allows a user to forward copies of the images or have other services for the images, consistently obtained from the same location without having to communicate with other vendors and without regard to the locations at which different images may have been scanned.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is block diagram illustrating a system of the present invention;

FIG. 2 is a data flow diagram illustrating the operation of some aspects of the system of FIG. 1;

FIG. 3 is a diagram illustrating the components of an identification generated for an associated image set signal; and

FIG. 4 is a block diagram illustrating a system of FIG. 1 with a further connection of the hub to another hub.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

EMBODIMENTS OF THE INVENTION

As can be seen, there is no teaching of a photo identification document. (Elsewhere Dellert speaks of using such imagery for greeting cards, or on cups and plates,[21] but again: nothing is said about photo identification documents.)

Because the rejection is premised on a mis-reading of Dellert, the Office has not met its burden of establishing *prima facie* obviousness of claim 3.

5. Claim 5 (§103 Dellert)

Claim 5 is allowable for its dependence from claim 1, and is also independently allowable. The claim reads:

> *5. The method of claim 1 in which the governmental agency is a motor vehicle licensing agency, and the image is a driver license photo.*

[21] *See, e.g.,* Dellert at col. 9, lines 42-45.

Conceding that Dellert does not teach such limitations, the Office sought to establish obviousness by dismissing the claim language as nonfunctional descriptive material:[22]

> 9. With respect to Claim 5, Dellert does not explicitly disclose the governmental agency is a motor vehicle licensing agency, and the image is a driver license photo. However these differences are only found in the nonfunctional descriptive material and are not functionally involved in the steps recited. The soliciting, receiving and printing would be performed the same regardless of the agency being a motor vehicle licensing agency and the image being a driver license photo. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, see In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983); In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994).

As noted above, "descriptiveness" is not a ground for ignoring language found in the claim. *All* claim limitations necessarily are descriptive – they serve to *describe* the claimed invention.

The Office cited the *Gulak* and *Lowry* cases in its rejection. The *Gulak* case does not support the rejection. In that case (which involved claims drawn to information stored on a computer-readable medium), the Federal Circuit *reversed* the Board, and held that the Office *should have given* patentable weight to the descriptive material (stored on the computer-readable medium).

Likewise in *Lowry*: the Federal Circuit *reversed* – holding that the Board erred by denying patentable weight to questioned claim limitations.

In the present case the claims are not drawn to a physical medium, but rather are *method* claims. The claimed acts, e.g., "soliciting" and "receiving," have no meaning without the nouns and adjectives appearing in the claim. Contrary to the Office's assertion, such terms are integrally, and functionally, involved in the recited acts. As was the case in *Gulack* and *Lowry*, it was error for the Office to disregard Appellant's claim limitations.

---

22 Final Rejection, page 4, second paragraph.

Again, the Office has not met its *prima facie* burden, and the rejection of claim 5 should be reversed.

6. Claim 10 (§103 Dellert)

Claim 10 stands or falls with the Dellert-based rejection of claim 1, from which it depends.

7. Claim 11 (§103 Dellert)

Claim 11 is an independent claim, and concerns the basic method of claim 1 but as practiced from the government agency side of the transaction:

> *11. A method of distributing a trusted image, comprising:*
> *at a governmental agency, receiving an electronic request for an archived personal image from an individual depicted in said image; and*
> *electronically transmitting said image to said individual.*

This claim stands or falls with the Dellert-based rejection of claim 1.

8. Rhoads 5,841,886

All of the remaining claims stand rejected over Dellert in view of Rhoads (5,841,886).

Rhoads (commonly-owned) discloses that an ID document (e.g., an identification badge) can be steganographically encoded with additional data. This data may include the name of a person depicted in the ID document photograph.

9. Claim 4 (§103 Dellert + Rhoads)

Claim 4 is allowable for its dependence on claim 1, and is also independently patentable. The claim reads:

> *4. The method of claim 1 in which said document is an identification badge.*

The claim is independently allowable because the rejection does not meet the Office's *prima facie* burden.

The rationale for combining the modified Dellert arrangement with the badge teaching of Rhoads is:

> One would be motivated to have this as identification badges are desirable and widely used for identification purposes (In Rhoads: Col. 1 lines 27-34 and Col. 6 lines 44-57).[23]

While it is true that identification badges are desirable and widely used for identification purposes, the rejection is silent as to why such teaching would have been combined with Dellert's online photo ordering method. The rejection makes an unexplained leap. It lacks the "articulated reasoning with some rational underpinning" required by *KSR*.

The rejection should be reversed.

---

[23] Final Rejection, page 5, middle of page.

10. Claim 6 (§103 Dellert + Rhoads)

Claim 6 is allowable for its dependence on claim 1, and is also independently patentable. The claim reads:

> *6. The method of claim 1 in which said image is processed with an identification code by the governmental agency.*

The rationale for combining the modified Dellert arrangement with identification-code teachings of Rhoads is:

> One would be motivated to have this, as it enhances the security of photo identification documents (In Rhoads: Col. 7 lines 4-11).[24]

While Rhoads enhances the security of photo identification documents, the Office again focuses on photo identification documents without any mention of same in Dellert - which concerns online photo ordering. Again, the rejection makes an unexplained leap – lacking the "articulated reasoning with some rational underpinning" required by *KSR*.

Again, the Final Rejection has not established *prima facie* obviousness.

11. Claims 7-9, 12-15 (§103 Dellert + Rhoads)

Claims 7-9 and 12-15 stand or fall with the Dellert + Rhoads based rejection of claim 6.

12. Claim 28 (§103 Dellert + Rhoads)

Claim 28 is allowable for its dependence on claim 1, and is also independently patentable. The claim reads:

> *28. The method of claim 1 that includes obtaining from a database maintained by said governmental agency a name of said individual user, and printing said obtained name on the document.*

---

[24] Final Rejection, top of page 6.

The rejection of claim 28 fails, for two reasons.

One is that – as with claim 6 – the Office has turned to Rhoads without any "articulated reasoning with some rational underpinning" for doing so.

A second reason is that the Office has mis-read Rhoads. The Final Rejection states:

> Rhoads teaches obtaining from a database a name of said individual user and printing said obtained name on the document (In Rhoads Col. 1 lines 46-67 and Col. 7 lines 30-54).

However, the cited passages do not teach the required claim limitations.[25]

Again, the Final Rejection has not established *prima facie* obviousness of claim 28.

---

[25] The two cited passages read:

An illustrative embodiment of the present invention is a method of correlating, with a photograph, information about an individual whose image appears in the photograph. The method includes steganographically encoding multi-bit information into the photograph. This encoding serves to add noise to the photograph--noise that is not generally perceptible as a representation of the multi-bit information except by computer analysis. (The encoded photograph appears to convey only an image of the individual to viewers of the photograph.) Sometime after encoding, the multi-bit information is decoded. Finally, some sort of authentication decision about the individual is made, based at least in part on the multi-bit information decoded from the photograph.

Another illustrative embodiment of the present invention is a substrate (e.g. a card, or a page from a magazine) with a photograph. The photograph is steganographically encoded with multi-bit data related to the photograph. This data is manifested as a slight snow effect that is not generally perceptible as a representation of the multi-bit data except by computer analysis. The multi-bit data can serve various purposes (e.g. identify an owner of the photograph; serve as a serial number index into a database, etc.).

and

In another embodiment of this aspect of the invention, the photograph component 1010 of the identification document 1000 may be digitized and processed so that the photographic image that is incorporated into the photo ID document 1000 corresponds to the "distributable signal" as defined above. In this instance, therefore, the photograph includes a composite, embedded code signal, imperceptible to a viewer, but carrying an N-bit identification code. It will be appreciated that the identification code can be extracted from the photo using any of the decoding techniques described above, and employing either universal or custom codes, depending upon the level of security sought.

It will be appreciated that the information encoded into the photograph may correlate to, or be redundant with, the readable information 1012 appearing on the document. Accordingly, such a document could be authenticated by placing the photo ID document on a scanning system, such as would be available at a passport or visa control point. The local computer, which may be provided with the universal code for extracting the identification information, displays the extracted information on the local computer screen so that the operator is able to confirm the correlation between the encoded information and the readable information 1012 carried on the document.

VIII. CONCLUSION

None of the rejections meets the Office's burdens. Accordingly, the Board is requested to reverse the Examiner and remand for issuance of a Notice of Allowance.

Respectfully submitted,

Date: April 18, 2008

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX 503-469-4777

By /William Y. Conwell/
William Y. Conwell
Registration No. 31,943

IX. CLAIMS APPENDIX

1. A method of printing a trusted image, comprising:

an individual user electronically contacting a governmental agency, soliciting an image depicting the user stored in an archive maintained by said governmental agency;

electronically receiving said image from said contacted governmental agency; and

printing a document incorporating said image.

2. The method of claim 1 in which it is the individual user who receives said image and prints said document.

3. The method of claim 1 in which said document is a photo identification document.

4. The method of claim 1 in which said document is an identification badge.

5. The method of claim 1 in which the governmental agency is a motor vehicle licensing agency, and the image is a driver license photo.

6. The method of claim 1 in which said image is processed with an identification code by the governmental agency.

7. The method of claim 1 in which said image is digitally watermarked with a plural-bit code by the governmental agency.

8. The method of claim 7 in which said plural-bit code serves to identify the individual user's name.

9. The method of claim 8 in which said plural-bit code comprises an index into a data structure in which the individual user's name is stored.

10. A document printed according to the method of 1.

11. A method of distributing a trusted image, comprising:

at a governmental agency, receiving an electronic request for an archived personal image from an individual depicted in said image; and

electronically transmitting said image to said individual.

12. The method of claim 11 that includes processing said image with an identification code prior to said electronic transmission.

13. The method of claim 11 that includes digitally watermarking said image with a plural-bit code prior to said electronic transmission.

14. The method of claim 13 in which said plural-bit code serves to identify the individual's name.

15. The method of claim 14 in which said plural-bit code comprises an index into a data structure in which the individual's name is stored.

16. (Withdrawn): A document printing method, comprising:

receiving a digital photo, the photo having plural-bit data steganographically encoded therein;

by reference to said steganographically encoded data, generating text to be printed with said photo; and

printing a document including both said photo and said text.

17. (Withdrawn): The method of claim 16 that includes electronically transmitting at least a part of said plural-bit data to a remote computer, and receiving the text from said computer.

18. (Withdrawn): The method of claim 16, that includes receiving said digital photo from an archive of facial images.

19. (Withdrawn): The method of claim 16 that includes receiving said digital photo from an image archive maintained by a government agency.

20. (Withdrawn): The method of claim 16 in which said document is an identification document.

21. (Withdrawn): A method of providing an access credential for a person, using a computer device for which the person is the proprietor, the method comprising:

receiving at said computer device code data, transmitted by an authority, the code data having a future time or date associated therewith;

steganographically encoding said code data in a graphic; and

presenting the encoded graphic as an access credential, to gain access to a restricted area.

22. (Withdrawn): The method of claim 21 that includes steganographically encoding said code data in said graphic using said computer device.

23. (Withdrawn): The method of claim 21 that includes printing said encoded graphic using a printer for which said person is also the proprietor, and presenting the printed graphic as said access credential.

24. (Withdrawn): The method of claim 21 in which the access credential authorizes entry to an event, the event taking place at said future time or date.

25. (Withdrawn): The method of claim 24 wherein the event is a movie.

26. (Withdrawn): The method of claim 21 that includes receiving said graphic from a governmental agency.

27. The method of claim 1 that includes printing said document at a home of said individual user.

28. The method of claim 1 that includes obtaining from a database maintained by said governmental agency a name of said individual user, and printing said obtained name on the document.

29. (Withdrawn): The method of claim 1 that includes:

using a computer operated by the individual user, extracting information steganographically encoded in the image received from the governmental agency;

transmitting said decoded information from said computer to a remote server;

in response, receiving name data corresponding to said decoded information from said remote server; and

printing said received name data on said document using said computer operated by the individual user.

30. (Withdrawn): The method of claim 1 wherein the received image has plural-bit data steganographically encoded therein, and the method includes:

by reference to said steganographically encoded data, generating text to be printed with said photo; and

printing a document including both said photo and said text.

31. (Withdrawn): The method of claim 1 that includes obtaining an access code from a corporation, and incorporating said access code on the printed document.

32. (Withdrawn): The method of claim 1 that further includes:

receiving code data at a home computer of said individual user, said code data having been transmitted by an authority, the code data having a future time or date associated therewith;

steganographically encoding said code data in said image received from said governmental agency; and

printing a document incorporating said steganographically encoded image.

33. A home-printed identification document produced by the method of claim 1.

34. (Withdrawn): A home-printed identification document produced by the method of claim 29.

35. (Withdrawn): A home-printed identification document produced by the method of claim 30.

36. (Withdrawn): A home-printed identification document produced by the method of claim 32.

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS APPENDIX

None